УДК 004.421, 004.912

ВЫЧИСЛЕНИЕ АВТОМАТНОЙ СЛОЖНОСТИ БУЛЕВЫХ ФУНКЦИЙ КАК ЗАДАЧА ДИСКРЕТНОЙ ОПТИМИЗАЦИИ

Н.И. Крайнюков, кандидат технических наук, доцент кафедры «Прикладная математика и информатика»

С.В. Пивнева, кандидат педагогических наук, доцент, доцент кафедры «Высшая математика и математическое моделирование»

Тольяттинский государственный университет, г. Тольятти (Россия)

Ключевые слова: булевы функции; недетерминированные конечные автоматы; конечно-автоматная сложность; дизъюнктивная нормальная форма.

Аннотация: Рассматривается задача вычисления сложности описания булевых функций с помощью дизъюнктивных нормальных форм, детерминированных конечных автоматов и упорядоченных двоичных разрешающих диаграмм. Рассмотрены примеры реализации функций тремя способами, проанализирована их сложность.

ВВЕДЕНИЕ

Булевы функции применяются во многих областях анализа дискретных систем, информатики. Компьютеры строятся на аппаратном обеспечении, в основе которого лежит булева алгебра – тип алгебры, в которой все переменные могут принимать только два значения: 0 и 1. Булева алгебра широко применяется в релейно-контактных схемах, транзисторах, цифровых вентилях и т.п.

Задача минимизации булевых функций может быть сформулирована следующим образом: найти представление заданной булевой функции в форме, содержащей минимально возможное число букв, в каком-то смысле минимальное. В общей постановке данная задача пока не решена, однако достаточно хорошо исследована в классе дизъюнктивно-конъюнктивных нормальных форм. Известно, что любая булева формула может быть приведена к дизъюнктивно нормальной форме (ДНФ). Для этого можно использовать закон двойного отрицания, закон де Моргана, закон дистрибутивности.

Используя законы булевой алгебры, можно получить для одной и той же логической функции множество эквивалентных представлений. Чем проще аналитическое выражение функции, тем экономичнее и проще ее практическая реализация на интегральных микросхемах.

Один из возможных способов задания булевых функций – с помощью конечных автоматов. Конечные автоматы являются моделью для многих компонентов аппаратного и программного обеспечения. Наиболее важные из них – это программное обеспечение, используемое для разработки и проверки цифровых схем, программное обеспечение для поиска в больших текстовых массивах, для проверки различного рода систем, которые могут находиться в конечном числе различных состояний, распознавание цепочек символов и т.п.

СЛОЖНОСТЬ БУЛЕВЫХ ФУНКЦИЙ И СЛОЖНОСТЬ КОНЕЧНЫХ АВТОМАТОВ

Сложность булевых функций – числовая характеристика булевых функций, выражающая трудность их вычисления. В частности, такой характеристикой (мерой сложности) может быть наименьшее число шагов, достаточное для вычисления данной функции в некотором классе алгоритмов, число функциональных элементов, достаточное для построения схемы, реализующей эту функцию, количество переменных в ее конъюнктивных или дизъюнктивных членах, количество элементарных конъюнкций в дизъюнктивной нормальной форме.

Наш подход, к определению сложности булевой функции $B(X)$ от $X = \{x_1, x_2, \ldots x_n\}$ n - переменных, состоит в следующем:

1. Выделяем те наборы $\tilde{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n) \in \{0,1\}$ для которых $B(x_1, x_2, \ldots x_n) = 1$, множество этих наборов будем определять конечный язык L_B.

2. Затем строим минимальный конечный автомат $A = (Q, \Sigma, \delta, i, F)$, с алфавитом $\Sigma = \{0,1\}$ допускающий язык L_A, такой, что $L_B = \Sigma^n \cap L_A$, где Q – конечное множество состояний, функция $\delta : Q \times \Sigma \to 2^Q$ переходов автомата, i – множество начальных состояний, F – множество заключительных состояний.

3. Каждому языку L_B ставится в соответствие минимально необходимое количество состояний, на которых можно построить конечный автомат, распознающий этот язык. Для детерминированного автомата (ДКА), такой автомат единственный, но для недетерминированного автомата (НДА), может существовать несколько различных НКА с минимально возможным количеством состояний, но само это количество для данного регулярного языка определяется однозначно.

4. Сложностью булевой функции $B(x_1, x_2, \ldots x_n)$ называется количество состояний автомата A. Будем называть эту величину ***автоматной*** *сложностью булевой функции* и обозначать $DBCom(B)$ (*deterministic Boolean complexity*) для детерминированного автомата A и $NDBCom(B)$ (*nondeterministic Boolean complexity*) для недетерминированного автомата A.

Рассмотрим несколько примеров реализации булевых функций с помощью ДНФ, информационных графов и конечных автоматов и сравним сложности их описания.

Пример 1. Рассмотрим функцию, заданную полиномом Жегалкина $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_6$. Это функция принимает значение 1 при $x_6 = 1$. При n=6 таких наборов 32.

В ДНФ-представлении эта функция имеет сложность, равную 1. Это можно проверить, составив СДНФ и сократив ее. Задав в системе GAP эту функцию, используя выражение *a_l:=ListOfWordsToAutomaton(),* получаем детерминированный конечный автомат, состоящий из 8-ми состояний:

a_l:=ListOfWordsToAutomaton(“01”,[“000001”,”000011”,”000101”,”000111”,”001001”,”001011”,”001101”,”001111”,”010001”,”010011”,”010101”,”010111”,”011001”,”011011”,”011101”,”011111”,”100001”,”100011”,”100101”,”100111”,”101001”,”101011”,”101101”,”101111”,”110001”,”110011”,”110101”,”110111”,”111001”,”111011”,”111101”,”111111”]);

```
< deterministic automaton on 2 letters with 8 states >
gap> Display(a_l);
  | 1 2 3 4 5 6 7 8
-----------------------------
 0 | 2 2 2 3 4 5 6 7
 1 | 2 2 1 3 4 5 6 7
Initial state:  [ 8 ]
Accepting state:  [ 1 ]
```

	1	2	3	4	5	6	7	8
0	2	2	2	3	4	5	6	7
1	2	2	1	3	4	5	6	7

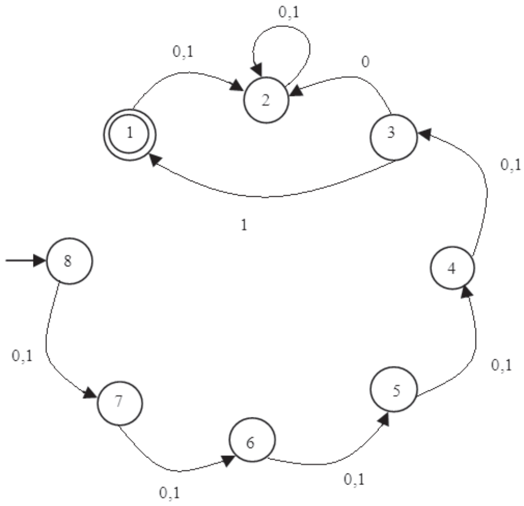


Рис. 1. Представление автомата функции $f(x_1,x_2,x_3,x_4,x_5,x_6)=x_6$

$(\{0|1\}^5 1)$ – регулярное выражение для этого автомата.

Данный автомат является минимальным, значит, в автоматном представлении сложность этой функции равна 8.

Построим упорядоченную двоичную разрешающую диаграмму для этой функции.

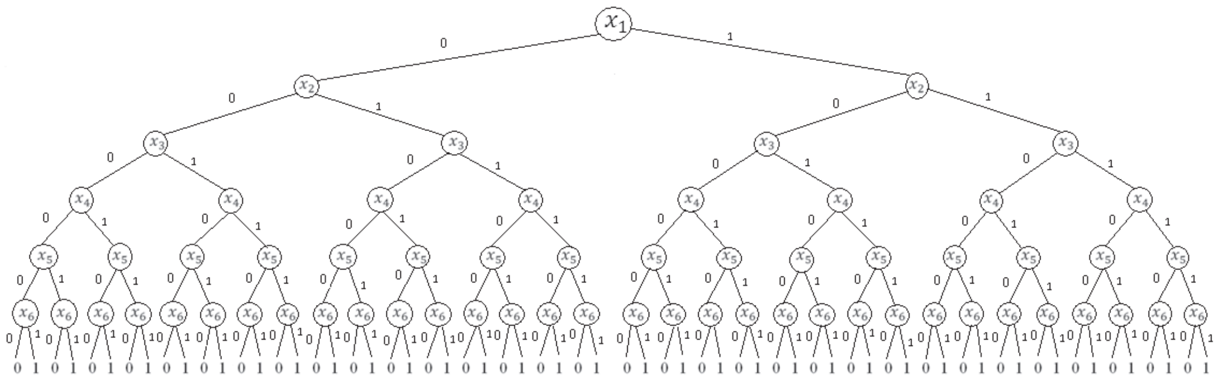
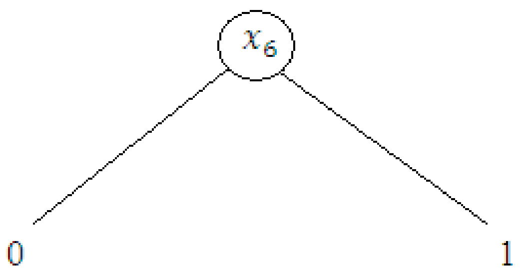


Рис. 2. Упорядоченная двоичная разрешающая диаграмма для функции $f(x_1,x_2,x_3,x_4,x_5,x_6)=x_6$.

Минимизировав эту диаграмму, получим:



	ДНФ-представление	Автоматное представление	Представление в виде упорядоченной двоичной диаграммы
Сложность	1	8	1

Рис. 3. Минимизированная диаграмма.

Пример 2. $f = x_5 \oplus x_6$

Минимизируя СДНФ получаем сложность функции в ДНФ-представлении равную 2. Автомат для этой функции будет иметь 9 состояний:

a_l:=ListOfWordsToAutomaton(“01”,[“000001”,”000010”,”000101”,”000110”,”001001”,”001010”,”001101”,”001110”,”010001”,”010010”,”010101”,”010110”,”011001”,”011010”,”011101”,”011110”,”100001”,”100010”,”100101”,”100110”,”101001”,”101010”,”101101”,”101110”,”110001”,”110010”,”110101”,”110110”,”111001”,”111010”,”111101”,”111110”]);

```
< deterministic automaton on 2 letters with 9 states >
gap> Display(a_l);
 | 1 2 3 4 5 6 7 8 9
--------------------------------
 0 | 9 9 1 2 4 5 6 7 9
 1 | 9 1 9 3 4 5 6 7 9
Initial state:  [ 8 ]
Accepting state:  [ 1 ]
```

	1	2	3	4	5	6	7	8	9
0	9	9	1	2	4	5	6	7	9
1	9	1	9	2	3	5	6	7	9

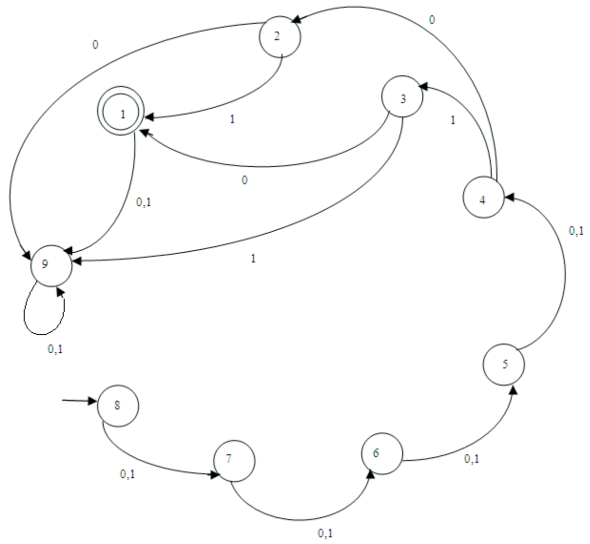


Рис. 4. Представление автомата функции $f = x_5 \oplus x_6$.

Построим упорядоченную двоичную разрешающую диаграмму для этой функции:

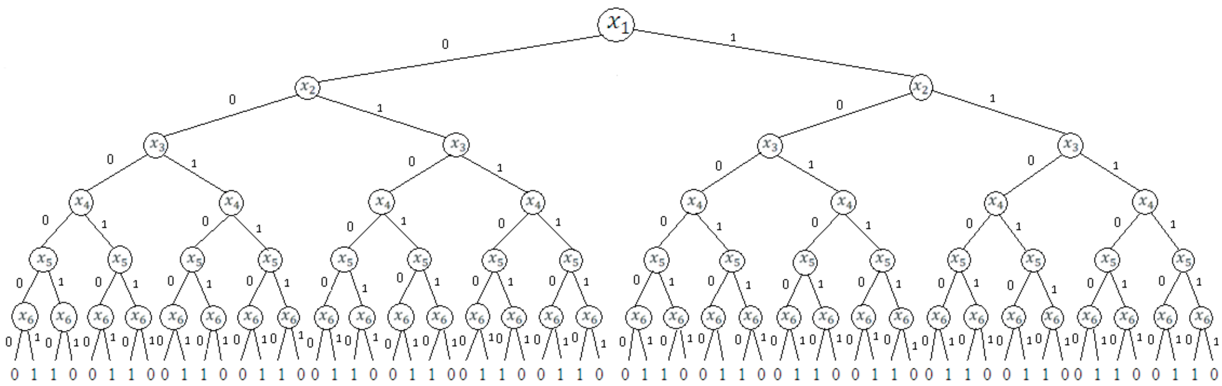
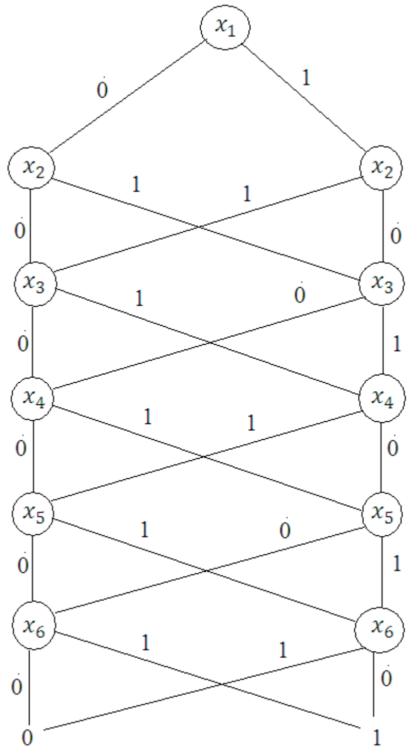


Рис. 5. Упорядоченная двоичная разрешающая диаграмма для функции $f = x_5 \oplus x_6$.

Минимальная OBDD:



	ДНФ-представление	Автоматное представление	Представление в виде упорядоченной двоичной разрешающей диаграммы
Сложность	2	9	11

Рис. 6. Минимизированная диаграмма.

Пример 3. В этом примере сгенерируем в GAPe произвольные наборы, на которых функция принимает значение 1.

Для начала с помощью функции Random зададим произвольное количество наборов, на которых функция принимает значение 1.

gap> kol_ed:=Random([1..64]);

44

Мы получили произвольное число 44.

gap> zn_ar:=[];

[ ]

Сгенерируем произвольные наборы.

gap> for i in [1..kol_ed] do Add(zn_ar, b6_L[Random([1..64])]); od;

gap> zn_ar;

[[0, 0, 0, 0, 0, 1], [1, 0, 0, 0, 1, 0], [1, 1, 0, 1, 1, 0], [1, 0, 1, 1, 0, 0], [1, 0, 1, 0, 0, 1],

[1, 1, 0, 0, 0, 1], [0, 1, 1, 0, 1, 1], [0, 0, 1, 0, 1, 1], [1, 0, 1, 0, 1, 0], [0, 0, 1, 1, 1, 1],

[1, 1, 1, 1, 0, 1], [1, 1, 0, 0, 1, 0], [0, 0, 1, 0, 0, 0], [1, 1, 1, 1, 1, 1], [1, 0, 1, 1, 0, 1],
[1, 0, 0, 1, 1, 1], [0, 1, 0, 1, 0, 0], [0, 1, 1, 0, 0, 1], [0, 1, 1, 1, 0, 1], [1, 1, 1, 0, 0, 1],
[1, 0, 0, 1, 1, 0], [1, 0, 0, 0, 1, 1], [1, 1, 0, 1, 0, 0], [1, 0, 1, 0, 0, 0], [0, 1, 0, 0, 1, 1],
[0, 0, 0, 1, 0, 0], [1, 1, 0, 1, 1, 1], [1, 0, 0, 0, 0, 1], [1, 1, 1, 0, 1, 1], [1, 0, 0, 0, 0, 0],
[1, 1, 0, 0, 1, 1], [1, 1, 0, 0, 0, 0], [0, 1, 1, 1, 0, 0], [1, 0, 0, 1, 0, 0], [0, 0, 0, 0, 1, 0],
[1, 0, 0, 1, 0, 1], [1, 0, 1, 0, 1, 1], [0, 0, 1, 0, 0, 1], [1, 1, 1, 0, 0, 0], [1, 1, 0, 1, 0, 1],
[0, 0, 1, 1, 0, 1], [1, 0, 1, 1, 1, 0], [1, 0, 1, 1, 1, 1], [0, 0, 1, 1, 0, 0]]

Составим СДНФ:

$$(\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}x_6) \cup (\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}\,\overline{x_6}) \cup (\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}\,\overline{x_6}) \cup (\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}\,\overline{x_6})$$
$$\cup (\overline{x_1}\,\overline{x_2}x_3\overline{x_4}\,\overline{x_5}x_6) \cup (\overline{x_1}\,\overline{x_2}x_3\overline{x_4}x_5x_6) \cup (\overline{x_1}\,\overline{x_2}x_3x_4\overline{x_5}\,\overline{x_6})$$
$$\cup (\overline{x_1}\,\overline{x_2}x_3x_4\overline{x_5}x_6) \cup (\overline{x_1}\,\overline{x_2}x_3x_4x_5x_6) \cup (\overline{x_1}x_2\overline{x_3}x_4x_5x_6)$$
$$\cup (\overline{x_1}x_2\overline{x_3}x_4\overline{x_5}\,\overline{x_6}) \cup (\overline{x_1}x_2x_3\overline{x_4}\,\overline{x_5}x_6) \cup (\overline{x_1}x_2x_3\overline{x_4}x_5x_6)$$
$$\cup (\overline{x_1}x_2x_3x_4\overline{x_5}\,\overline{x_6}) \cup (\overline{x_1}x_2x_3x_4\overline{x_5}x_6) \cup (x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}\,\overline{x_6})$$
$$\cup (x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}x_6) \cup (x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4}x_5\overline{x_6}) \cup (x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4}x_5x_6)$$
$$\cup (x_1\overline{x_2}\,\overline{x_3}x_4\overline{x_5}\,\overline{x_6}) \cup (x_1\overline{x_2}\,\overline{x_3}x_4\overline{x_5}x_6) \cup (x_1\overline{x_2}\,\overline{x_3}x_4x_5\overline{x_6})$$
$$\cup (x_1\overline{x_2}\,\overline{x_3}x_4x_5x_6) \cup (x_1\overline{x_2}x_3\overline{x_4}\,\overline{x_5}\,\overline{x_6}) \cup (x_1\overline{x_2}x_3x_4\overline{x_5}\,\overline{x_6})$$
$$\cup (x_1\overline{x_2}x_3\overline{x_4}x_5\overline{x_6}) \cup (x_1\overline{x_2}x_3\overline{x_4}x_5x_6) \cup (x_1\overline{x_2}x_3x_4\overline{x_5}x_6)$$
$$\cup (x_1\overline{x_2}x_3x_4\overline{x_5}x_6) \cup (x_1\overline{x_2}x_3x_4x_5\overline{x_6}) \cup (x_1\overline{x_2}x_3x_4x_5x_6)$$
$$\cup (x_1x_2\overline{x_3}\,\overline{x_4}\,\overline{x_5}\,\overline{x_6}) \cup (x_1x_2\overline{x_3}\,\overline{x_4}\,\overline{x_5}x_6) \cup (x_1x_2\overline{x_3}\,\overline{x_4}x_5\overline{x_6})$$
$$\cup (x_1x_2\overline{x_3}\,\overline{x_4}x_5x_6) \cup (x_1x_2\overline{x_3}x_4\overline{x_5}\,\overline{x_6}) \cup (x_1x_2\overline{x_3}x_4\overline{x_5}x_6)$$
$$\cup (x_1x_2\overline{x_3}x_4x_5\overline{x_6}) \cup (x_1x_2\overline{x_3}x_4x_5x_6) \cup (x_1x_2x_3\overline{x_4}\,\overline{x_5}\,\overline{x_6})$$
$$\cup (x_1x_2x_3\overline{x_4}\,\overline{x_5}x_6) \cup (x_1x_2x_3\overline{x_4}x_5x_6) \cup (x_1x_2x_3x_4\overline{x_5}x_6)$$
$$\cup (x_1x_2x_3x_4x_5x_6)$$

Приведем СДНФ к ДНФ:

$$(x_1\overline{x_2}x_3) \cup (x_1x_2x_3x_6) \cup (x_1x_2\overline{x_3}\,\overline{x_4}) \cup (x_1\overline{x_2}\,\overline{x_3}x_4) \cup (x_1x_2x_3x_4) \cup (\overline{x_1}\,\overline{x_2}x_3\overline{x_5})$$
$$\cup (x_1x_2x_3\overline{x_4}x_5) \cup (x_1x_2\overline{x_3}x_4\overline{x_5}) \cup (\overline{x_1}x_2x_3x_4\overline{x_5}) \cup (\overline{x_1}x_2x_3\overline{x_4}x_6)$$
$$\cup (\overline{x_1}\,\overline{x_2}x_3x_5x_6) \cup (\overline{x_1}\,\overline{x_3}x_4\overline{x_5}x_6) \cup (\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}x_6) \cup (\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}\,\overline{x_6})$$
$$\cup (\overline{x_1}x_2\overline{x_3}\,\overline{x_4}x_5x_6) \cup (x_1x_2x_3\overline{x_4}\,\overline{x_5}\,\overline{x_6})$$

В ДНФ-представлении сложность будет равна 16.

Напишем полином Жегалкина по этой таблице истинности:

$$P = x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_5 \oplus x_1x_6 \oplus x_2x_3 \oplus x_2x_5$$
$$\oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_6 \oplus x_1x_2x_3 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_5$$
$$\oplus x_1x_3x_6 \oplus x_2x_3x_4 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_5x_6 \oplus x_3x_5x_6$$
$$\oplus x_4x_5x_6 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_5x_6$$
$$\oplus x_1x_3x_5x_6 \oplus x_1x_4x_5x_6 \oplus x_2x_4x_5x_6 \oplus x_3x_4x_5x_6 \oplus x_1x_2x_3x_4x_5$$
$$\oplus x_1x_2x_3x_4x_6 \oplus x_1x_2x_3x_5x_6 \oplus x_1x_2x_4x_5x_6 \oplus x_1x_3x_4x_5x_6$$
$$\oplus x_2x_3x_4x_5x_6$$

По сгенерированным наборам в системе GAP получим ДКА:

gap>

a_l:=ListOfWordsToAutomaton(“01”,[“000001”,”100010”,”110110”,”101100”,”101001”,”110001”,”011011”,”001011”,”101010”,”001111”,”111101”,”110010”,”001000”,”111111”,”101101”,”100111”,”010100”,”011001”,”011101”,”111001”,”100110”,”100011”,”110100”,”101000”,”010011”, ”000100”,”110111”,”100001”,”111011”,”100000”,”110011”,”110000”,”011100”,”100100”,”000010”,”100101”,”101011”,”001001”,”111000”,”110101”,”001101”,”101110”,”101111”,”001100”]);

< deterministic automaton on 2 letters with 25 states >

gap> MinimalizedAut(a_l);

< deterministic automaton on 2 letters with 25 states >

Этот автомат задается таблицей переходов:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	25	25	1	3	16	5	6	10	18	9	19	4	23	5	2	3	4	15	2	1	20	25	22	3	25
1	25	25	1	2	16	5	14	7	17	13	24	19	11	12	20	3	4	21	2	25	25	2	21	25	25

Сложность автомата равна 25.

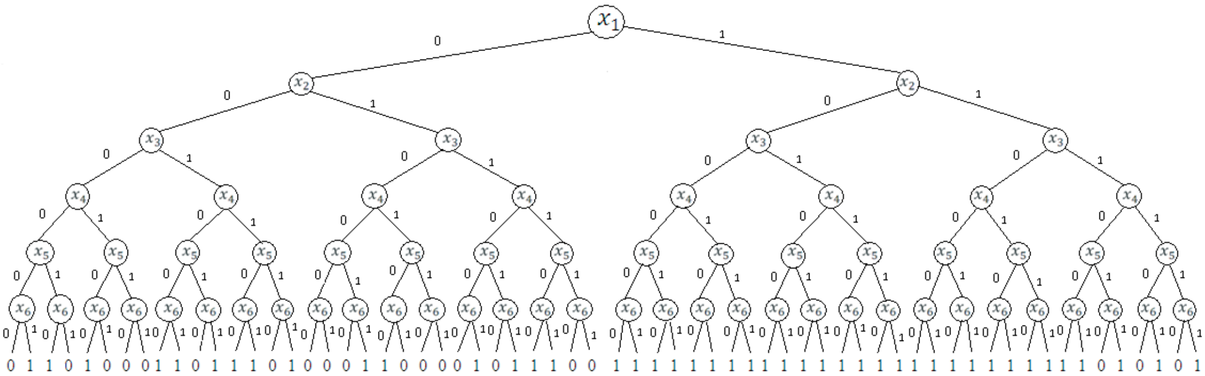
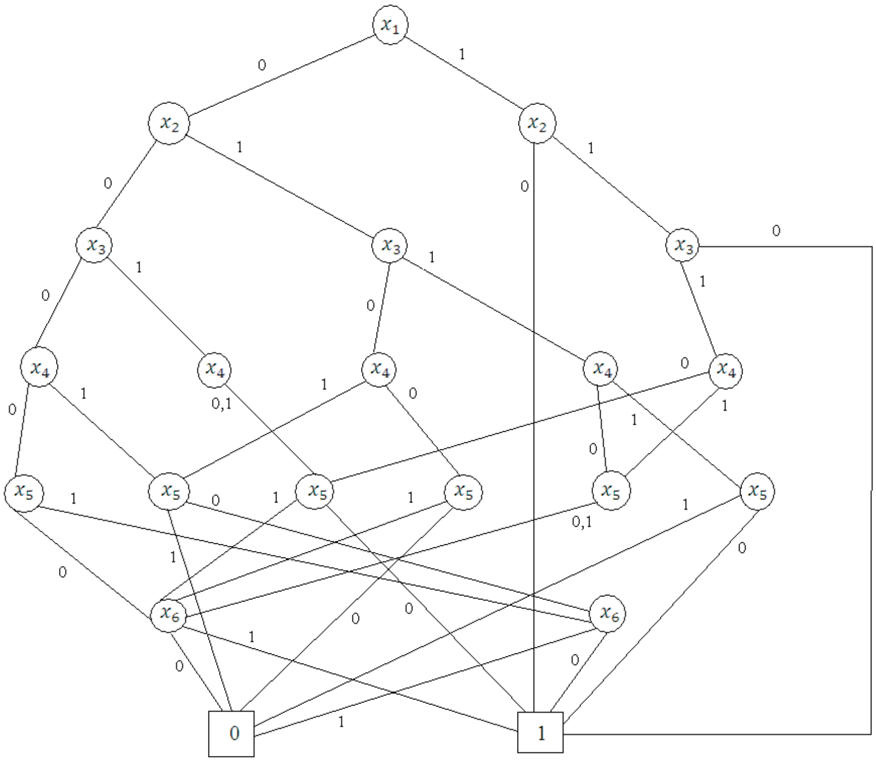


Рис. 7. Упорядоченная двоичная разрешающая диаграмма.

Минимальная упорядоченная двоичная разрешающая диаграмма:



	ДНФ-представление	Автоматное представление	Представление в виде упорядоченной двоичной разрешающей диаграммы
Сложность	16	25	19

Рис. 8. Минимизированная диаграмма.

Примеры показывают, что определение сложности булевой функции многоплановое понятие, в различных прикладных областях можно использовать различные подходы для этого.

Для вычисления автоматной сложности булевой функции приходится решать сложные задачи минимизации ДКА и НДА, последняя задача является (PSPACE-полной) и для булевых функций от большого количества переменных необходимо применение эвристических алгоритмов, например описанных в [7].

ЗАКЛЮЧЕНИЕ

Итак, в статье проанализирована сложность описания булевых функций с помощью ДНФ, конечных автоматов и упорядоченных двоичных разрешающих диаграмм. Показано, что понятие сложности различных представлений булевых функций взаимосвязаны и дополняют друг друга.

СПИСОК ЛИТЕРАТУРЫ

1. Мельников Б.Ф. Эвристики в программировании недетерминированных игр. – «Программирование» (Известия РАН), 2001, №5, С.63–80.
2. Пивнева С.В. Моделирование задач дискретной оптимизации / С. В. Пивнева, М. А. Трифонов // Вектор науки. – № 3 (13). – Тольятти : Тольят. гос. ун-т, 2010. – С. 31–34.
3. Пивнева С.В. Программная реализация задач дискретной оптимизации / С. В. Пивнева, М. А. Трифонов // Некоторые вопросы математического моделирования дискретных систем : сб. науч. тр. – Тольятти : ТГУ, 2011. – С. 210–219.
4. Поваров Г. Конечные трансдьюсеры и недетерминированная сложность регулярного языка. Известия вузов. Математика. 2010, № 6, С. 23–31.
5. Хопкрофт Дж., Мотвани Р., Ульман Дж.. Введение в теорию автоматов, языков и вычислений. 2-е изд.: Пер. с англ. – М. : Издательский дом «Вильямс», 2002. – 528 с. : ил. – Парал. тит. англ.
6. Шуткин Ю. Асимптотически оптимальная реализация булевых функций информационными графами. Дискрет. матем., 2011, 23:4, С.80–102.
7. Мельников Б. Мультиэвристический подход к задачам дискретной оптимизации. Кибернетика и системный анализ (НАН Украины), 2006, № 3, С. 32–42.

Работа частично поддержана программой Министерства образования и науки РФ в рамках Госзадания Тольяттинского государственного университета на 2012 год (шифр 6.3072.2011) и реализации гранта федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы (Соглашение № 14.B37.21.1934)

CALCULATION OF AUTOMATON COMPLEXITY OF BOOLEAN FUNCTIONS AS DISCRETE OPTIMIZATION PROBLEMS

N.I. Kraynyukov, candidate of pedagogical sciences, associated professor of the chair «Applied mathematics and informatics

S.V. Pivneva, candidate of pedagogical sciences, associated professor, associated professor of the chair «Higher mathematics and mathematical modeling»

Togliatti State University, Togliatti (Russia)

Keywords: Boolean functions; certainly-automatic complexity; final automatic devices.

Annotation: The problem of calculation of complexity of the description булевых functions by means of the disjunctive normal forms, the determined final automatic devices and the ordered binary diagrams is considered. Examples of realization of functions are considered by three ways, their complexity is analysed.

УДК 512.531.2

ПЕРЕБОРНЫЕ АЛГОРИТМЫ ПОДСЧЁТА ЧИСЛА КОНЕЧНЫХ ПОЛУГРУПП – ПОСТАНОВКА ЗАДАЧИ И ПРОСТЕЙШИЕ ЭВРИСТИКИ

Е.И. Кузичкина, аспирант

Тольяттинский государственный университет, Тольятти (Россия)

Ключевые слова: конечная полугруппа; алгоритмы перебора; эвристические алгоритмы.

Аннотация: Рассмотрены простые эвристические переборные алгоритмы для подсчёта числа конечных полугрупп.